



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,479	02/22/2002	Siani Lynne Pearson	B-4517 619563-3	8505

22879 7590 07/14/2006

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER
----------

AUGUSTIN, EVENS J

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**MAILED**

JUL 14 2006

**GROUP 3600**

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 10/080,479  
Filing Date: February 22, 2002  
Appellant(s): PEARSON ET AL.

---

Alessandro Steinfl  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed on 04/03/06 appealing from the Office action mailed on 10/30/2005.

**(2) Related Appeals and Interferences**

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Pending Appeal for U.S. S/N 09/979,903 ("Data Integrity Monitoring In trusted Computed Entity") is related to the present appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

No amendment after final has been filed.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

6,327,652

England et al.

12-2001

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

***Status of Claims***

Art Unit: 3621

1. Claims 1-10 and 12-24 have been examined.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) The invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-10 and 12-24 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (U.S 6,327,652).

As per claims 1-10 and 12-24, England et al. discloses a computer system that identifies computers in a network comprising of the following:

- A server (column 8, line 43) that makes challenges to user devices accessing content within a network (column 9, lines 41-51). The challenges can take place when certificates have to be renewed periodically (column 12, lines 37-40). A log or historical status of the user devices in the network is also being kept (column 13, lines 54-59), and the content of the log must be certified when the device is challenged (column 14, lines 38-39). The content provider server also stores (or keep record) of an “access predicate”, which the server makes available with the content and the “access predicate” contains response specifications that must be reconciled during access (column 19, lines 6-40) –

*Claims 1, 2, 9, 21, 23, 24*

- Keeping a log or historical status of the user devices in the network (column 13, lines 54-59), and the content of the log must be certified when the device is challenged (column 14, lines 38-39) – *Claim 3*
- Response message transmitted to the server, that includes the identity of the user devices (new or used) (column 9, lines 48-51) – *Claims 4-5*
- In the challenge-response process (column 9, line 52), the content will not be accessed unless a trust relationship is established between the devices (column 10, lines 14-17) – *Claims 6-7,*
- The server is the main hub (gateway) of access of content for a particular content provider (figure 1) - *Claim 8*
- The “access predicate” contains unique identifiers that must be provided during access of the digital content (column 19, lines 15-39) - *Claim 10*
- The user-computing device (figure 1a, item 20) contains a processing unit (figure 20, item 21), arranged as part of a network to send and receive information (item 1a, items 51, 52). Information/content will not be accessed unless a trust relationship is established between the devices (column 10, lines 14-17) – *Claim 12*
- The user-computing device (figure 1a, item 20) contains a processing unit (figure 20, item 21), arranged as part of a network to send and receive information (item 1a, items 51, 52). Information/content will not be accessed unless a trust relationship is established between the devices (column 10, lines 14-17). The challenge-response process follows common protocols for data exchange (column 9, lines 52-55) – *Claims 13, 22*

Art Unit: 3621

- Counters can be used as part of a challenge as to whether or not a certificate is not valid or untrustworthy (column 12, lines 43-52, column 15, lines 50-60, column 19, lines 45-49) – *Claims 14-15*
- Making challenges to user devices accessing content within a network (column 9, lines 41-51). The challenges can take place when certificates have to be renewed periodically (column 12, lines 37-40). Storing (or keep record) of an “access predicate”, associated with the digital content and containing response specifications that must be reconciled during access (column 19, lines 6-40) – *Claims 16, 17*
- Keeping a log or historical status of the user devices in the network (column 13, lines 54-59), and the content of the log must be certified when the device is challenged (column 14, lines 38-39) – *Claim 18*
- The response message transmitted to the server and includes the identity of the user devices (new or used) (column 9, lines 48-51) - *Claim 19*
- The “access predicate” contains unique identifiers that must be provided during access of the digital content (column 19, lines 15-39), in order to establish a trust relationship (column 10, lines 14-17) – *Claim 20*

#### **(10) Response to Argument**

##### **Argument #1:**

Prior Art does not teach the aspect of a trusted computer...keeping a record of the response

**Response #1:**

Trust, as it relates to computing environment, is the aspect of having reassurance that the devices within that particular computing environment are operating the way they are intended to, and have not been tempered with (appellant's specification page 2, lines 12-14). According to the appellant's specification, the reassurance of trust within a computing environment is done through a challenge/response protocol within the devices. Accordingly, the prior art by England et al. teaches a computing environment in which the devices are authenticated via challenge/response protocol. In this case, a content provider (server) authenticates the user requesting the content via user devices through challenge/response protocol (column 9, lines 45-50). The computer environment is a networked environment, of comprising of devices such as computer, server, network computer, a router and/or another common network node (column 6, lines 56-57). The network can be a local-area network, a wide-area network such as the internet (column 7, lines 1-4). Before content is downloaded from the content provider to the user requesting the content, the content provider (Note: content provider/third party/operating system vendor or used interchangeably by the prior art – column 19, lines 4-5) performs a validation process of the user/device. The validation process includes the recording of the user computer's identity and checking frequency of the requests (challenge/response protocol accompanies every request) made by the user (column 18, lines 26- 33), by the content provider/server. The user's identity is sent as part of the response form the user computer (column 9, lines 48-51). Note: DRMOS, as referred to in the prior art, is synonymous with user device - To prevent their content from being stolen or misused, content providers will download content only to known software, and therefore only to subscriber computers that can prove that their operating systems

Art Unit: 3621

will enforce the limitations the provider places on the content. Such a digital rights management operating system (DRMOS) must load and execute only OS components that are authenticated as respecting digital rights ("trusted"), and must allow access to the downloaded content by only similarly trusted applications (column 8, lines 56-65).

**Argument #2:**

Prior art does not teach the aspect of making records available.

**Response #2:**

The content provider records the identity of user device, as part of the validation process, before content is sent to the user (column 18, lines 30-33). The content provider examines the user's devices identity before it determines the establishment of a trust relationship (column 9, lines 65-67, column 10, lines 1-3). The user's identity is part of every challenge/response protocol (column 9, lines 48-51).

**Argument #3:**

Prior art does not the aspect of listening to communication between, in order to identify to new devices.

**Response #3:**

The prior art's invention takes place in a distributed computing environment via communication networks (devices listening to each other) (col. 5, lines 57-60), such as the internet (col. 7, line 4). When a request is made, the content provider responds to the request through challenge/response. Part of that process is to identify the user computer (col. 9, lines 41-50).



**Argument #4:**

Prior art does not teach the aspects of a response/challenge Identifier within the challenge/response to verify the validity of challenge/response.

**Response #4:**

Part of the response by the user device includes a rights manager certificate (col. 9, lines 49-51), which gets renewed or authenticated periodically (col. 12, lines 39-40). The rights manager certificate is reconciled with an “access predicate” at the server end (column 10, lines 41-51). There are properties in the rights manager certificate that must be reconciled before a trust relationship is established (response rules) (column 9, lines 65-67, column 10, lines 1-3).

**Argument #5:**

Prior art does not teach the aspect of a user device capable of examining whether the challenge is coming from a trusted device

**Response #5:**

The challenge from the content provider is asking for the identity of the user device, the identity of the digital rights management software requesting the content (DRMOS) (column 9, lines 45-47). To prevent their content from being stolen or misused, content providers will download content only to known software, and therefore only to subscriber computers that can prove that their operating systems will enforce the limitations the provider places on the content. Such a digital rights management operating system (DRMOS) must load and execute only OS components that are authenticated as respecting digital rights ("trusted"), and must allow access

Art Unit: 3621

to the downloaded content by only similarly trusted applications (column 8, lines 56-65).

Therefore, the DRMOS allows the user device to effectuate the trust relationship between the user device and the content provider.

**Argument #6:**

Prior art does not the aspect of checking the level of trust

**Response #6:**

Processes are performed by components of user devices and content providers/servers (col. 8, lines 45-47). Before a component gets loaded to the user device, it checks the trust level of component (column 4, line 8, column 12, lines 26-27).

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Evens Augustin

Patent Examiner – Art Unit 3621

Conferees:

Sam Sough – Supervisor Patent Examiner 3628

  
Pierre Elisca – Primary Examiner 3621

Application/Control Number: 10/080,479

Page 10

Art Unit: 3621

Evens Augustin - Examiner 3621

*Ev-j*